

Google Geofence Guide

Main Concepts –

1. Android and some iPhones will report location related data back to Google when powered on. This reporting of location information cannot be disabled by the user.
2. The frequency of this reporting will vary from every second to 5+ minutes, depending on the device activity at the time.
3. This data is sourced from information received by the phone in reference to known cell towers, known available WiFi connections, and GPS. The device does not have to connect to the WiFi to generate this location information, nor does the WiFi on the device have to be on.
4. Google will assign an “anonymized” number to a device. This number is known as a Device ID.
5. Google never deletes the Device ID location data.
6. Google may not be able to provide any further information on the Device ID other than the Device ID. If a user has deleted their account information, all that remains is the Device ID. End users cannot delete the Device ID location information, because it is maintained and stored in an anonymous state.
7. Under the stored communication act (18 U.S.C. 2703) this data is available to law enforcement through the issuance of a probable cause search warrant (Comply with Carpenter v United States requiring a warrant to obtain cell site location information).

What does all of this mean? Hypothetically, if a suspect has an Android device and went to a location where there is a WiFi connection that is known to Google, the phone may probe that WiFi connection while the device is in close proximity to the WiFi connection. Google would be able to provide a list of Device ID(s) that saw that WiFi connection at a given date and time. Additionally, if the phone reported it's GPS, that information would also be available. Cell tower data (although not generally as accurate through Google) may also be available.

To request this information from Google, you need two pieces of information –

1. A general location. This is the “geofence” piece of the warrant. This is the geographical area that you want Google to search for the presence of a device that reported location information. The “geofence” can be defined to Google in one of two ways –

- a. A polygon shape with the latitude and longitude of each point of the polygon. For example, if you drew a square over the area you wanted search, provide Google with the latitude and longitude of each corner of the square.
 - b. A latitude and longitude point with a given radius. For this location, simply provide the latitude and longitude of your scene/location to be searched and then a radius (provided in meters), given latitude xx.xxxxxx, given longitude -xx.xxxxxx, and a 50 meters radius.
 - c.
2. A timeframe. While this is typically focused on the time of the crime, it is important to request a Significant enough data set to be able to determine what devices are regularly seen in the area and “belong” there, to be used as a control sample. By identifying those devices, it is easier to isolate suspicious devices that may be related to the crime.

Attached is a Google Geofence Search Warrant template that incorporates the applicable information.

This guide is intended to assist in the initial warrant process only. Please review our tutorial video of “Understanding Google” for more information.

Downers Grove Police

Email

Date: 01/14/19
No. of pages including cover sheet:

To: Google Legal Investigations Support
ATTN:
Phone: 844-383-8524
Email: uslawenforcement@google.com
CC:

From: Robert Bylls
Email: rbylls@downers.us
Phone: 6303646003
Fax Phone: 6304345690

[Type here]

Warrant # _____

**IN THE DUPAGE COUNTY SUPERIOR COURT
COUNTY OF DUPAGE, STATE OF IL**

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A
SEARCH WARRANT**

STATE OF IL)
)
COUNTY OF DUPAGE)

Your Petitioner, **Robert Bylls**, a Peace Officer of the **Downers Grove Police Department**, being duly sworn, upon oath, deposes and says that:

REMARKS: Urgent For your review Reply ASAP Please Comment
--

If your agency is registered with Google's Law Enforcement Response System (LERS), upload the approved search warrant into LERS. If not -

Email - uslawenforcement@google.com

For Custodian of Records and Legal Investigations Support call the "Emergency Disclosure Request" department at: 650-253-3425.

Leave a message and an agent will call you back. For search warrant requests, please send them to: Email: USLawEnforcement@google.com (preferred by Google) or by Fax: 650-249-3429.

****WARNING****

The information transmitted by this facsimile is considered CONFIDENTIAL and is intended only for the use of the individual or entity named. If the reader of this message is not the intended recipient, or the employee/agent responsible to deliver it to the intended recipient, you should be aware that any dissemination, distribution or copying of this communication is STRICTLY PROHIBITED. If you receive this communication in error, please immediately notify us by telephone, and return the original message to the above listed address via U.S. Postal Service. Thank you.

[Type here]

1. I make this affidavit in support of an application for a search warrant for information that is stored at premises controlled by Google, a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in **Attachment A**. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(b)(1)(A), (add any applicable State statutes) and there is probable cause to require Google to disclose to the government copies of the information further described in **Attachment B**.
2. I am a [Title] with the Downers Grove Police Department and have been since [[DATE]]. [DESCRIBE TRAINING AND EXPERIENCE TO THE EXTENT IT SHOWS QUALIFICATION TO SPEAK ABOUT THE CRIMES UNDER INVESTIGATION AND RELEVANT TECHNICAL MATTERS.]
3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of [STATUTES] have been committed by [SUSPECTS or unknown persons]. There is also probable cause to search the information described in **Attachment A** for evidence of these crimes further described in **Attachment B**.

JURISDICTION

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711 (3)(B). Specifically, the Court a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.”

BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY

[Type here]

5. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. Cellular telephones send signals through networks of transmitter/receivers called “cells,” enabling communication with other cellular telephones or traditional “landline” telephones. Cellular telephones rely on cellular towers, the location of which may provide information on the location of the subject telephone. Cellular telephones may also include global positioning system (“GPS”) technology for determining the location of the device, as well as known WiFi locations identified by the device.
6. Google is an Internet company which, among other things, provides electronic communication services to subscribers. Google allows subscribers to obtain email accounts at the domain name gmail.com. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.
7. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s

[Type here]

user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

8. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.
9. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling your affiant to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. Further, information maintained by the email provider can show how, where, and when the account was accessed or used. Based on my training and experience, I have learned that Google also maintains records that may reveal other Google accounts accessed from the same electronic device, such as the same computer or mobile device, including accounts that are linked by Hypertext Transfer Protocol (HTTP) cookies, which are small pieces of data sent from a website and stored in a user's Internet browser.

[Type here]

10. Google has developed an operating system for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account and users are prompted to add a Google account when they first activate a new Android device.
11. Based on my training and experience, I have learned that Google collects and retains location data from Android-enabled mobile devices. The company uses this information for location-based advertising and location-based search results. This information is derived from sources including GPS data, cell site/cell tower information, and Wi-Fi access points.
12. Location data can assist investigators in understanding the chronological and geographic context of the email account access and device usage relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email).

PROBABLE CAUSE

13. **[PC Statement Goes Here]**
14. **[Explain why your PC is linked to the information provided in Attachment A. For example, explain that your particular crime occurred in the specific geographical location that has been geofenced in exhibit as and the crime was committed during the period of time specified.]**

CONCLUSION

[Type here]

- 15.** Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Robert Bylls

SUBSCRIBED and SWORN to before me this 01/14/19

Judge

Warrant # _____

ATTACHMENT A

Property to Be Searched

This warrant is directed to Google LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, and applies to (1) GPS, WiFi or Bluetooth sourced location history data generated from devices that reported a location within the geographical region bounded by the following latitudinal and longitudinal coordinates, dates, and times ("Initial Search Parameters") and (2) identifying information for Google Accounts associated with the responsive location history data:

[Type here]

- Date and Time Period (Provided in **XX** Time Zone):
 - Start Time: **mm/dd/yyyy hh:mm**
 - End Time: **mm/dd/yyyy hh:mm**
- Target Location: Geographical area identified as
 - o **[option 1: a radius of N meters around a latitude/longitude coordinate in the format xx.xxxxxx, -xx.xxxxxx]**
 - o **[option 2: a polygon defined by at least three latitude/longitude coordinates in the format xx.xxxxxx, -xx.xxxxxx connected by straight lines]**

[Type here]

Warrant # _____

ATTACHMENT B

Items to Be Seized And Searched

Information to be disclosed by Google

Google shall provide responsive data (as described in **Attachment A**) pursuant to the following process:

1. Google shall query location history data based on the Initial Search Parameters (as described in **Attachment A**).
2. For each location point recorded within the Initial Search Parameters, Google shall produce anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the "Anonymized List").
3. Law enforcement shall review the Anonymized List to remove devices that are not relevant to the investigation, for example, devices that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the Time Period that fall outside of the Target Location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the Target Location, were not within the Target Location for a long enough period of time, were moving through the Target Location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

[Type here]

4. For those device IDs identified as relevant pursuant to the process described above, law enforcement may request that Google Provide identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each identified device ID.

[Type here]

Warrant # _____

Search Warrant

IN THE DUPAGE COUNTY SUPERIOR COURT COUNTY OF DUPAGE, STATE OF IL

Account and Location Information

TO ANY PEACE OFFICER IN THE STATE OF IL:

Proof having been made before me by Robert Bylls that:

1. The matter supported by affidavit is a legitimate matter for law enforcement inquiry, this search warrant is made pursuant to: 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), 2703(c)(1)(A) and 2703(c)(2) (insert applicable State statutes here) and there is probable cause to believe that the crime of Armed Robbery has been committed and the information being sought is evidence of that crime.

Subject Accounts and Execution of Warrant

2. This warrant is directed to Google, Inc. (the "Provider"), headquartered at 1600 Amphitheatre Parkway, and applies to all content and other information within the Provider's possession, custody, or control associated with the Google accounts located within the geographical region bounded by the following latitudinal and longitudinal coordinates between (Time Period listed in Attachment A - mm/dd/yyyy hh:mm time zone and mm/dd/yyyy hh:mm time zone) (the "Subject Accounts"):

Geographical range defined by:

[Type here]

Insert geofence parameters from exhibit A here

INFORMATION TO BE PROVIDED BY GOOGLE

To the extent within Google's possession, custody, or control, Google is directed to produce the following information associated with the Subject Accounts, which will be reviewed by law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by Google in order to locate any evidence, fruits, and instrumentalities of [State Code and crime being investigated].

1. ***Location information.*** All location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings, between [time range identified in Attachment A].
2. Each device corresponding to the location data to be provided by Google will be identified only by a numerical identifier, without any further content or information identifying the user of a device. Law enforcement will analyze this location data to identify users who may have witnessed or participated in the Subject Offenses and will seek any additional information regarding those devices through further legal process.
3. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the "Provider" shall provide additional location history outside of the predefined area for those relevant accounts to determine path of travel. This additional location history shall not

[Type here]

exceed 60 minutes plus or minus the first and last timestamp associated with the account in the initial dataset. (The purpose of path of travel/contextual location points is to eliminate outlier points where, from the surrounding data, it becomes clear the reported point(s) are not indicative of the device being within the scope of the warrant.)

4. For those accounts identified as relevant to the ongoing investigation through an analysis of provided records, and upon demand, the “Provider” shall provide the subscriber’s information for those relevant accounts to include, subscriber’s name, email addresses, services subscribed to, last 6 months of IP history, SMS account number, and registration IP.

Which said property is subject to search and seizure as set out by the Laws of [STATE] for the following grounds, to wit:

A PUBLIC OFFENSE BEING COMMITTED, TO WIT: **List crime and statute**

Due to the sensitivity of this on-going criminal investigation, the notification to the listed subscribers by Google, Inc. (the “Provider”) that these records have been released to a law enforcement agency could compromise this investigation as well as the safety of law enforcement officers participating in the investigation. Based on these facts, it is further ordered that the customer/subscriber is not to be notified of the release of this information, as it could jeopardize an on-going criminal investigation.

Furthermore, pursuant to 18 U.S.C 3124(d), no cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with this court order.

[Type here]

YOU ARE THEREFORE COMMANDED at any time of the day to make an immediate search of the records of Google, Inc. (the “Provider”), located and described as follows, to wit:

This warrant is directed to Google, Inc. (the “Provider”), headquartered at 1600 Amphitheatre Parkway, and applies to all content and other information within the Provider’s possession, custody, or control associated with the Google accounts located within the geographical region bounded by the following latitudinal and longitudinal coordinates between **[time range provided in Attachment A]** (the “Subject Accounts”):

Geographical range defined by:

Insert geofence parameters from exhibit A here

These services can be accessed within **[County and State]**. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711 (3)(B). Specifically, the Court a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants.”

Given under my hand and dated this _____ day of _____, 20

Judge